



Cyber Attack Readiness and Response Cheat Sheet.

for corporate counsel

For trends, see the **EY Global Information Security Survey 2021**: 77% of the respondents (2020: 59%) warn that they have seen an increase in the number of disruptive attacks, such as ransomware, over the last 12 months. Only 9% of boards (20%) are extremely confident in their organization's cybersecurity measures. <https://go.ey.com/3UyM1Bx>

	Before	In the first 72 hours	Thereafter	Noteworthy
 <p>Security & Forensics</p>	<ul style="list-style-type: none"> Make IT security a top priority in all your technical and organizational processes Have an integrated Intrusion Detection System and enough resources to analyze daily alerts Make sure your systems are patched on a regular basis and don't forget your operational technology environment, vendors and third parties Prepare offline backups for critical Systems and don't forget to regularly test them Make sure your employees understand phishing and CEO fraud patterns Regularly test your cyber incident response and BCM plan through role play 	<ul style="list-style-type: none"> Setup a "war room" with clear roles and responsibilities and include your external partners and international stakeholders Make sure you have main Leads in the following key areas: (1) Overall Incident Lead, (2) IT & Incident Response and Forensic, (3) Communication, (4) Legal & Compliance Scoping, gaining visibility and understanding the attack (ideally with a fully integrated artefact collection solution) can be key for a timely response Get expert guidance if crypto ransom payments are involved Take immediate steps to remediate an attack but be careful to document and stay aligned 	<ul style="list-style-type: none"> Restore systems and data in a prioritized way and make sure the restored data has been cleaned of potential malware Analyze all accounts (also admins) and change passwords to make sure the perpetrator is out Analyze hacker access to critical databases and check for changes made by an intruder (do you know for how long your system has been compromised?) If data was breached, get assistance to understand what information is out in the open (e.g., from your Darknet monitoring) Make sure to do a broad security assessment to understand why the attack was possible 	<ul style="list-style-type: none"> In the case of a cyber incident, the first finding is often that the emergency plan is outdated, communication channels are unavailable and the people responsible are no longer in the company Intrusion Detection Systems (IDS) are often not rolled out broadly enough (e.g., not for shadow IT systems) or they generate too many false positive alerts to be monitored efficiently Incident reporting to the top management is important but avoid overloading the technical experts with too many reporting requests Monitor your systems for months after the attack to detect any "sleepers" in the system
 <p>Legal & Compliance</p>	<ul style="list-style-type: none"> Have a data breach notification policy that sets forth responsibilities (including local vs central) Have old, unneeded data/files/copies deleted securely, including by your service providers Know, for each entity who has to be notified of a data breach or attack, when and how; also keep in mind contractual obligations and other jurisdictions where you do business Know the data that could expose you or third-parties most if lost or stolen, where it is stored and how it can be identified Retain a law firm with experience Draft business contracts to protect and not expose you in case you are hit by an attack Do a data protection impact assessment prior to using tools that monitor IT usage (e.g., EDR) 	<ul style="list-style-type: none"> Find out which (critical) data may have been stolen, if any, and how it could be abused Identify the key jurisdictions affected Do not only think of personal data, but also any third-party secrets you are to protect Check thresholds for notifications required by law (to regulators, individuals) or by contract (business partners) and notify them as needed within the deadlines (e.g., EEA/UK: 72h) Inform employees quickly; consider voluntary info of customers, key partners and the media Be candid, but avoid details, admission of fault Document key decisions and the assessments Get outside counsel, preserve legal privilege Consider involving the police cyber crime unit Have the Darknet monitored for your data 	<ul style="list-style-type: none"> Document all data breaches (even low risk) Document damage incurred (costs, additional time spent by staff, lost business) Consider issuing a litigation hold Update your assessments; do follow-up notifications to regulators and key partners Consider raising claims against those providers that bear responsibility for the data breach or failed business contingency measures (if any) Defend against regulatory action Defend against civil action Defend against criminal proceedings Make provisions and tax deductions (damage, ransom), issue profit warnings, as applicable Update policies and other organizational measures based on the lessons learned 	<ul style="list-style-type: none"> Data stolen in attacks often turns out to be data that the victim should have deleted long ago, which can result in additional issues Notifications may have to be in local language Manual or automated data reviews can help you better understand what data has been stolen; the 80:20 approach is usually sufficient Many victims make ransomware payments, as this is ultimately a business decision; it is often possible to negotiate, but do not talk about it Good communication to your stakeholders is key and can protect against long-term effects Test your organization in a mock-up attack Proving indirect damages is very difficult You may also be subject to foreign data breach laws if you serve foreign markets
 <p>Insurance</p>	<ul style="list-style-type: none"> Have a cyber incident insurance policy that covers all relevant risks (e.g., loss of data) Retain a cyber incident consultant Have the insurance policy available offline Understand your obligations according to your cyber insurance policy 	<ul style="list-style-type: none"> Notify your insurance co. without undue delay Carefully comply with all other obligations according to your cyber insurance policy Document any measures taken Add your inhouse legal counsel to the incident response team (cyber insurances are complex) 	<ul style="list-style-type: none"> All internal costs must be documented by a statement of work and not only by timesheets If there is chance of insurance coverage litigation, find and retain an external coverage counsel who is not conflicted 	<ul style="list-style-type: none"> Insurers will deep dive into any violations of terms, conditions and obligations in claims notification and co-operation duties to avoid or limit payment Ransom can be covered by insurance, if negotiated

In cooperation with:



Contacts:

Security & Forensics Adrian Ott, adrian.ott@ch.ey.com, +41 79 768 76 38, Ernst & Young AG
Legal & Compliance David Rosenthal, drosenthal@vischer.com, +41 79 322 10 38, VISCHER Ltd.
Insurance Helmut Studer, helmut.studer@kessler.ch, +41 44 387 87 17, Kessler & Co AG

